

REMARKS

The Examiner has objected to Claim 8. Applicant respectfully asserts that such rejection is moot in view of the cancellation of such claim.

The Examiner has rejected Claims 1-8, 17-24 and 33-40 under 35 U.S.C. 102(e) as being anticipated by Ackroyd (U.S. Patent Application Number 2002/0131256). The Examiner has further rejected Claims 9-16, 25-32 and 41-48 under 35 U.S.C. 103(a) as being unpatentable over Ackroyd in view of Moore et al. (U.S. Patent Application No. 2003/0120947). Applicant respectfully disagrees with such rejections, especially in view of the amendments made hereinabove to each of the independent claims. Specifically, applicant has amended each of the independent claims to incorporate the subject matter of dependent Claims 2-5, 7 and 9 et al. along with additional language which further distinguishes the foregoing references.

With respect to the subject matter of dependent Claim 5 et al., presently incorporated into each of the independent claims, the Examiner has relied on paragraphs [0027]-[0029] and [0032] in Ackroyd to make a prior art showing of applicant's claimed technique "wherein the level of the malware event comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected."

After a careful review of such excerpts relied on by the Examiner, applicant notes that Ackroyd merely teaches that "generated reports are compared with predetermined patterns and network-wide thresholds" such that if the "thresholds have been exceeded or patterns matched," then "anti-malware actions are triggered." Applicant further notes that the thresholds and patterns disclosed in Ackroyd relate to a number of events detected (see specifically paragraph [0032] lines 6-9). Clearly, determining whether a

number of events meets a threshold does not meet applicant's claimed "level of the malware event" (emphasis added), where the malware event is defined as claimed.

Still yet, the Examiner argues that "the determination of whether or not operator intervention is necessary is inherent of the ability to determine whether or not the number of malware detections is significant." Applicant respectfully disagrees. Ackroyd specifically teaches "predetermined patterns and network-wide thresholds held in a store." Clearly, comparing a number of malware detections with predetermined thresholds would allow for an automated determination of whether the number of malware events was significant, and thus operator intervention would not be required.

In view of the above arguments, Ackroyd clearly fails to teach or even suggest applicant's claimed technique "wherein the level of the malware event comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected." Further, any inherency argument made by the Examiner has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements, is respectfully requested. (See MPEP 2112)

With respect to the subject matter of dependent Claim 7 et al., presently incorporated into each of the independent claims, the Examiner has again relied on paragraphs [0027]-[0029] and [0032] in Ackroyd to make a prior art showing of applicant's claimed technique "wherein the level of the event trigger threshold comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected." For substantially the same reasons as

argued above with respect to the subject matter of dependent Claim 5 et al., applicant respectfully asserts that the Ackroyd reference fails to meet applicant's specific claim language.

With respect to the subject matter of dependent Claim 9 et al., presently incorporated into each of the independent claims, the Examiner has relied on paragraph [0034] from Moore to make a prior art showing of applicant's claimed technique "wherein the transmitting step comprises the steps of: transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold."

Applicant respectfully asserts that such excerpt from Moore relied on by the Examiner merely teaches that "[i]f malware has been identified, then...one or more malware found actions are triggered....[including] issuing a warning message concerning the computer file, for example to the user, the system administrator or the AV product provider..." However, applicant notes that such excerpt fails to specifically teach that the warning is transmitted in real-time, as claimed by applicant. Furthermore, nowhere in the Moore reference is there even a suggestion of "transmitting the notification of the detected malware event eventually," as claimed by applicant (emphasis added).

In addition, the Examiner argues that it would have been obvious to incorporate the malware found transmitting actions of Moore into the system of Ackroyd to meet applicant's specific claim language. Applicant respectfully asserts that both Ackroyd and Moore only teach triggering events upon the detection of malware (Moore) and upon a threshold or pattern being met (Ackroyd). However, neither reference teaches triggering an event eventually "if the level of the detected malware event is less than the event trigger threshold," as specifically claimed by applicant (emphasis added).

Applicant also emphasizes the incorporation of the following claim language into each of the independent claims which further distinguishes the prior art of record:

“wherein the event trigger threshold is configurable to control an amount of the notifications that are received in real-time.”

Applicant respectfully asserts that nowhere in the Moore or Ackroyd reference is there any disclosure of a configurable event trigger threshold that is capable of being configured to control an amount of notifications that are received in real-time.

With respect to the 102 rejection, the Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.* 868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim. This criterion has simply not been met by the Ackroyd reference, for the reasons argued below.

With respect to the 103 rejection, and to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991). Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, for the reasons argued above.

Thus, in view of the substantial amendments made hereinabove to each of the independent claims, a notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Thus, the applicant respectfully submits that claims 1-8, 17-24, and 33-40 are not anticipated by Ackroyd, and that claims 9-16, 25-32, and 41-48 are not obvious over the combination of Ackroyd and Moore.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 49-81 below, which are added for full consideration:

“wherein the event trigger threshold is set at a management server in a malware management program” (see Claim 49 et al.);

“wherein the event trigger threshold is set by setting policies in the malware management program” (see Claim 50 et al.);

“wherein the event trigger threshold is distributed to a plurality of malware agents residing in a plurality of user systems” (see Claim 51 et al.);

“wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until an eventual periodic event transmission” (see Claim 52 et al.);

“wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until a request by a management server is received” (see Claim 53 et al.);

“wherein the level of the event trigger threshold is selected from a ranked set of levels including, from least critical to most critical with progressively greater levels, as follows:

- (1) the informational malware events requiring no operator intervention;
- (2) the warning malware events that indicate a process failure;
- (3) the minor malware events that require attention, but are not events that could lead to loss of data;
- (4) the major malware events that need operator attention; and
- (5) the critical malware events that need immediate operator attention and could lead to loss of data if not corrected” (see Claim 54 et al.);

“wherein the completion of the malware scan corresponds to one of the informational malware events requiring no operator intervention” (see Claim 55 et al.);

“wherein the process failure relating to the malware scanning corresponds to one of the warning malware events that indicate a process failure” (see Claim 56 et al.);

“wherein the missing log file corresponds to one of the minor malware events that require attention, but are not events that could lead to loss of data” (see Claim 57 et al.);

“wherein the detection of the malware corresponds to one of the major malware events that need operator attention” (see Claim 58 et al.); and

“wherein the failure of the response to the malware corresponds to one of the critical malware events that need immediate operator attention and could lead to loss of data if not corrected” (see Claim 59 et al.).

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

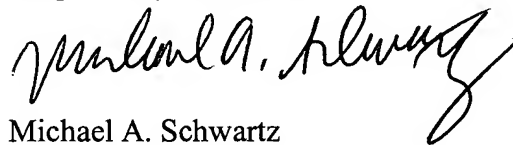
Additional Fees:

The Commissioner is hereby authorized to charge any insufficient fees or credit any overpayment associated with this application to Deposit Account No. 19-5127 (19903.0016).

Conclusion

In view of the foregoing, all of the Examiner's rejections to the claims are believed to be overcome. The Applicants respectfully request reconsideration and issuance of a Notice of Allowance for all the claims remaining in the application. Should the Examiner feel further communication would facilitate prosecution, he is urged to call the undersigned at the phone number provided below.

Respectfully Submitted,

A handwritten signature in black ink, appearing to read "Michael A. Schwartz", written in a cursive style.

Michael A. Schwartz
Reg. No. 40,161

Dated: November 10, 2005

Swidler Berlin, LLP
3000 K Street, N.W., Suite 300
Washington, D.C. 20007
(202) 424-7500